INDIANA DATA

AND

COMMUNICATIONS SYSTEM

IDACS NCIC AUDIT PROCEDURES MANUAL

TABLE OF CONTENTS

Introduction

Objectives

General Scope of the Audit

Methodology

IDACS Sanctions

Administrative Compliance Requirements

System Security Compliance Requirements

Missing Person File Compliance Requirements

Vehicle File Compliance Requirements

Vehicle File Risk Analysis

Wanted Person File Compliance Requirements

Wanted Person File Risk Analysis

Non-Terminal Agency Administrative Compliance Requirements

Audit Forms

Introduction

The NCIC Advisory Policy Board (APB) at their October, 1984 meeting, mandated that each state implement certain initiatives to enhance record quality in IDACS/NCIC. That by December 31, 1986 each CTA shall establish a system to biennially audit every terminal agency to ensure compliance with state and NCIC policy and regulations.

Subsequently, IDACS has implemented the same basic inspection and audit procedures that are followed by NCIC during their biennial audit.

Objectives

1. To review and document compliance with applicable laws, regulations, policies, and procedures.

2. To be alert for situations or transactions that could be indicative of fraud, abuse, illegality, or cause unnecessary risk to civil liabilities.

3. To recommend areas for improvement of IDACS operations both at the control terminal and local level.

4. To obtain pertinent views of responsible officials from audited agencies.

5. To obtain a description of noteworthy accomplishments particularly when local management accomplishments may be beneficial to other agencies.

General Scope of the Audit

1. Terminal Agency Coordinator Responsibilities.
2. Quality, accuracy, and timeliness of Wanted File entries.
3. Validations Procedures.
4. Record availability.
5. Hit Confirmation Procedures.
6. Audit Trail Requirements.
7. Use of appropriate ORI's.
8. User Agreements.
9. Security of terminal, access, personnel, and data.
10. Criminal History Audit Trails, dissemination, and use.
11. Management Control Requirements for Computer and Dispatch Centers.
12. Missing Person File Compliance Requirements.
13. Vehicle File Compliance Requirements and Risk Analysis.
14. Wanted Person File Compliance Requirements and Risk Analysis.
15. Non-Terminal Agency Compliance Requirements.

16. Data Quality Review

Methodology

Audits will be conducted at each IDACS terminal agency about once every two years. Non-terminal agencies will be audited if determined that problems exist for which the responsible terminal agency cannot correct.

1. IDACS Security Officers whenever possible will pre-schedule audit dates that are mutually acceptable with the terminal agency coordinator.

2. The on-site phase of the audit will consist of a review of each of the listed areas to ensure that there is compliance.

3. The auditor will then check specific wanted file records, criminal history requests, and other system transactions, to determine the extent of compliance with data quality, validation, audit trails, and other appropriate requirements.

4. Upon completion, the auditor will review the results of the inspection with an agency official.

5. The auditor will report to the IDACS Chairman any serious violations, for possible review by the whole Committee and/or recommend sanctions. See IDACS Sanctions later in this manual.

6. As necessary, follow-up visits will be done to determine the

progress on any recommended improvements.

IDACS Sanctions

240 IAC 5-2-12 User agency sanctions

Authority: IC 10-1-1-3; IC 10-1-2.5-7
Affected: IC 5-2-5-5; IC 10-1-2.5-2

Sec. 12. (a) The IDACS committee shall review violations of IDACS rules and make recommendations to the state police superintendent to impose sanctions on user agencies.

(b) The objectives of the sanction procedure shall be as follows:
(1) To ensure the integrity of the SYSTEM
(2) Create an awareness among user agencies of the importance of following rules, regulations, and procedures in order to minimize the risk to liabilities that may be incurred by misuse of the SYSTEM and its data.

(c) Sanctions shall be based upon the class of violation, any previous violations, and any exposure to criminal and civil liabilities that the violation might place on the SYSTEM, its officials, and the offending agency.

(d) Violations shall be classed as either Administrative (minor) or Security (serious) Violations. Security Violations being defined as one which has or could result in access of SYSTEM data by unauthorized individuals. All other Violations are classed as Administrative.

(e) In determining the severity of the Violation, the violation type, either Administrative or Security, and previous sanctions issued, if any, shall be considered. The IDACS Committee may impose as sanctions one of the following:

(1) Verbal Warning
(2) Written Warning
(3) Written Notice of Violation
(4) Written Notice of Probation
(5) Written Notice of Temporary Suspension
(6) Written Notice of Permanent Suspension

(f) Temporary or permanent suspension of service will not begin, unless an emergency exists, until fifteen (15) days after the Agency Head has received written notice by certified mail or personal service.

(g) An Agency may after one (1) year apply to be reinstated if placed on permanent suspension.
(State Police Department; filed Aug 6, 1990, 4:40 PM)

SECTION A
ADMINISTRATIVE
COMPLIANCE REQUIREMENTS

1. NCIC and IDACS requires that each agency have a designated Terminal Agency Coordinator (TAC), with the below listed responsibilities.

   (1) Ensure that all agency personnel (including any nonterminal agencies serviced) utilizing system information are aware of the

rules and policies of the IDACS/NCIC/NLETS system.

(2) Disseminate the contents of the IDACS/NCIC newsletters to all terminal operators, and maintain copies for three (3) years.

(3) Ensure that validation reports are properly processed.

(4) Ensure that terminal operators receive proper IDACS training in accordance with the IDACS certification training program.

(5) Maintain NCIC and IDACS Operating Manual and NCIC Code Manual revisions and disseminate information to operators.

(6) Advise IDACS of any changes in the agency head, the coordinator, agency address, or terminal site.

(7) Report all IDACS rule violations and other improper uses to IDACS.

(240 IAC 5-2-8, IDACS Manual Part I, Section G.)

2. Accuracy is essential as is promptness in entering, modifying, locating, or clearing records in the system. Each record on file is identified with the agency originating that record and that agency alone is responsible for the accuracy, completeness, and correct status of that record at all times. IDACS cannot assume responsibility for the accuracy of any records entered by any agency. (Compliance will be determined in data quality review).

   (240 IAC 5-1-1, IDACS Manual Part I, Section D.)

3. The accuracy of IDACS/NCIC records must be double-checked by a second party. That verification should include assuring that the available cross-checks, e.g., VIN/License Numbers, were made, and that data in the NCIC record matches the data in the investigative report.

   Agency agrees to abide by accepted quality assurance methods. This includes compliance with validation procedures as specified in the Indiana Administrative Code, NCIC serious error procedures, and IDACS quality control procedures. Agency further agrees to establish local procedures whereby updates to the wanted files are reviewed for accuracy by comparing the update with supporting documentation. This comparison shall be made by a person other than the operator who accomplished the update and the investigating officer who ordered it.

(240 IAC 5-2-9 IDACS User Agency Agreement)

4. All IDACS user agencies shall validate, on a periodic basis, as prescribed to the user agency by IDACS, all IDACS wanted records entered on their authority. Validation of records shall be in conformity and compliance with rules set forth by IDACS.

   a. Validation obligates the originating agency to confirm the record is COMPLETE, ACCURATE and is still OUTSTANDING or ACTIVE. Validation is accomplished by reviewing the original entry and current supporting documents and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual. In the event the originating agency is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority shall make a determination based on the best information and knowledge available whether or not to retain the original entry on file.

   b. Validation procedures must be formalized and copies of these procedures must be on file for review during an IDACS or NCIC audit.

   (240 IAC 5-2-7, IDACS Manual Part I Section F.)

5. Terminal agency agrees to ensure that hit confirmation is available twenty-four (24) hours a day on records entered into the wanted files. This includes being able to provide a substantive response to an inquiry within ten minutes.
   (240 IAC 5-2-9 IDACS User Agency Agreement)

6. Originating agency has an obligation to supply a substantive response within (10) minutes to the inquiring agency This response shall include a confirmation or denial of the wanted notice, or the length of time it will take to respond.
   (240 IAC 5-1-1, IDACS Manual Part I Section D, Part II Section A.)

7. When an agency receives a positive response (wanted notice) from IDACS or NCIC, an immediate follow-up confirmation request with the agency that originated the record in the system is necessary before any enforcement action is taken. Confirming a hit means to contact the agency that entered the record to:

   Ensure that the person or property inquired upon is identical to the person or property identified in the record;

   Ensure that the warrant, missing person report, or theft report is still outstanding; and

   Obtain a decision regarding (1) the extradition of a wanted person, (2) information regarding the return of the missing person to the appropriate authorities, or (3) information regarding the return of stolen property to its rightful owner.

   (240 IAC 5-1-1, IDACS Manual Part I Section D.)

8. When an operational inquiry ("Q") on an individual or property yields a valid positive response (hit), the terminal-produced printout showing the inquiry message transmitted and the record(s) on file in IDACS/NCIC should be retained for use in documenting probable cause for the detention of the missing person, arrest of the wanted person, or seizure of the property. The printout may also prove valuable in a civil suit alleging a false arrest, a false imprisonment, a civil rights violation, or an illegal seizure of property. When an IDACS/NCIC inquiry yields a hit, the terminal employee making the inquiry should note on the terminal-produced printout precisely how, when, and to whom the information was given; initial and date this notation; and forward the printout to the inquiring officer or agency for retention in the case file.

   (240 IAC 5-1-2, IDACS Manual Part I Section D.)

9. Every agency upon taking a person into custody or acquiring property, after confirming the hit, must place a locate on the corresponding IDACS/NCIC record(s).

   (IDACS Manual Part II, Sections B-J)

10. An inquiry of any IDACS/NCIC File must contain a valid ORI in the ORI Field. Agencies making inquiries for another agency must use the ORI of the other agency.
(NCIC Manual 13-7, Para 1.5, IDACS Manual Part I, Section I.)

11. All IDACS user agencies shall complete a "user agreement" before utilizing the system. Agencies with terminals and statutory police agencies shall complete such agreements with the Indiana state police and the IDACS committee. Non-terminal agencies shall complete an agreement with the terminal agency that services them.
(240 IAC 5-2-9, IDACS Manual Part I, Section C.)

12. Any criminal justice agency or regional dispatch center may act as holder of the record for a criminal justice agency and such criminal justice agency or regional dispatch center may place its own ORI in the ORI Field only when there is a written assignment between the two (2) agencies delegating the legal responsibilities for the record. Responsibilities for the record include entering and updating the record, confirming a hit on the record, and removing the record from file. Any agency that does not have a written agreement must store in the ORI Field of the record the valid NCIC assigned ORI of the agency requesting transmission of the entry. (There may not be any of these kind of arrangements in Indiana).
(NCIC Manual 13-7, Para 1.5)

SECTION B
SYSTEM SECURITY
COMPLIANCE REQUIREMENTS

1. All agencies and computer centers having terminals on the SYSTEM and/or

having access to SYSTEM data shall physically place these terminals in a secure location previously approved by the IDACS Committee within the authorized agency. Subsequent physical location changes of terminals shall have prior approval of the IDACS Committee.
(240 IAC 5-2-10 J (3), IDACS Manual Part I, Section C.)

2. It is incumbent upon an agency operating an IDACS terminal to implement the necessary procedures to make that terminal secure from any unauthorized use.

Access, meaning the ability to obtain information from the System, shall be permitted only to criminal justice agencies in the discharge of their official mandated responsibilities, and those agencies as required by state and/or federal enabling authority. Release of Indiana bureau of motor vehicles data to noncriminal justice agencies may occur when it is determined to be in the best interest of law enforcement/criminal justice to do so. Agencies that shall be permitted access to SYSTEM data include the following:

(1) Police forces and departments at all governmental levels (including private college and railroad police departments as authorized by Indiana Code) that are responsible for enforcement of general criminal laws.

(2) Prosecutive agencies and departments at all governmental levels.

(3) Courts at all governmental levels with a criminal or equivalent jurisdiction.

(4) Correction departments at all governmental levels, including corrective institutions and probation departments.

(5) Parole commissions and agencies at all governmental levels.

(6) Agencies at all governmental levels which have as a principal function the collection and provision of fingerprint identification information.

(7) Regional or local governmental organizations established pursuant to statute which collect and process criminal justice information and whose policy and governing boards have, as a minimum, a majority composition of members representing criminal justice

agencies.
(240 IAC 5-2-10 b, IDACS Manual Part I, Section C.)

3. The agencies having terminals with access to SYSTEM data shall have terminal operators screened and restrict access to the terminal to a minimum number of authorized employees.

   ...they shall be screened thoroughly under the authority and supervision of the IDACS committee or their designated representative. This screening shall also apply to noncriminal justice maintenance or technical personnel. The screening process shall consist of a character investigation, including fingerprints, for the purpose of establishing suitability for the position. Investigations shall consist of the gathering of information as the applicant's honesty, integrity and general reputation. Personal characteristics or habits, such as lack of judgment, lack of physical or mental vigor, inability to cooperate with others, intemperance, or other characteristics which would tend to cause the applicant to be unsuitable for this type of position, shall be considered sufficient grounds for rejection. Also, convincing information in an applicant's past history involving moral turpitude, disrespect for law, or unethical dealings shall be considered sufficient grounds for rejection. If any of the above facts are presented to the IDACS committee, a recommendation shall be made and presented to the state police superintendent for a final approval or disapproval decision.
   (240 IAC 5-2-10 j (3)(B), IDACS Manual Part I, Section C.)

4. Copies of SYSTEM data obtained from terminal devices shall be afforded security to prevent any unauthorized access to or use of that data. Copies of SYSTEM data which are no longer relevant shall be destroyed.
   (240 IAC 5-2-10 j (1)(C), IDACS Manual Part I, Section C.)

5. Established IDACS committee policy requires all user agencies to an audit trail for six (6) months for certain types of IDACS transactions as itemized but not limited to the following:

(1) Switched Messages (both transmitted and received).
(2) Bureau of motor vehicles and department of natural resources information file data.
(3) IDACS/NCIC stolen file data.
(4) Out-of-State (NLETS) Bureau of motor vehicles or department of natural resources data.

These audit records shall include, but are not limited to, the names of all persons or agencies to whom the information is disseminated and the date and time upon which such information is disseminated. Audit trails shall be maintained manually or by automation, and shall be made available to the IDACS committee for inspection upon request. It should be noted that these are minimum requirements and it may be necessary to keep important or case related traffic for longer periods of time in order to properly confirm or validate IDACS/NCIC wanted entries.

(240 IAC 5-1-2, IDACS Manual Part I, Section D.)

6. Title 28 United States Code states that audits shall be kept pertaining to the dissemination of criminal history records. This includes responses from NCIC's Interstate Identification Index (NCIC III) and responses from state central repositories and other agency criminal history files (both in-state and out-of-state). Such audit records shall include, but are not limited to, the names of all persons or agencies to whom the information is disseminated and the date and time upon which such information is disseminated. These shall be kept for at least one (1) year.

   (240 IAC 5-1-3, IDACS Manual Part I, Section D.)

7. Audio response terminals, radio devices, and mobile data terminals, whether digital (teleprinters) or voice, shall not be used for the transmission of criminal history data beyond that information necessary to effect an immediate identification or to ensure adequate safety for officers and the general public. Transmission shall be made to police officers upon his or her request.

   (240 IAC 5-2-10 (3)(D), IDACS Manual Part I, Section C.)

8. Criminal history and Violent Gang/Terrorist data on an individual from the national computerized file shall be made available outside the federal government to criminal justice agencies for criminal justice purposes. This precludes the dissemination of such data for use in connection with licensing (except when a federal, state, or local law/ordinance exists making the criminal justice agency responsible for the processing or issuing of the licenses/permits) applications, or local or state employment, other than with a criminal justice agency, or for other uses unless such dissemination is pursuant to state and federal statutes or state and federal executive order. There are no exceptions.
(240 IAC 5-2-10 (h)(1), IDACS Manual Part I, Section C.)

9. Inquiries and record requests transmitted to the III (and to state repositories must include the purpose for which the information is to be used.

A. Criminal Justice (Purpose Code "C") Ä must be used when the transaction is for official duties in connection with the administration of criminal justice.

B. Criminal Justice Employment (Purpose Code "J") Ä must be used when the transaction involves employment with the previously described authorized agencies.

C. Firearms (Purpose Code "F") - must be used when processing an appliction for purchase of a firearm, and/or an application for a license to carry a handgun.
(IDACS Manual Part VII, Section B,C.)

REGIONAL COMPUTER INTERFACES & CENTRALIZED DISPATCHES

10. All computers, electronic switches, and manual terminals (including mobile data terminals/printers) interfaced with the SYSTEM computer for

the exchange of SYSTEM data shall be under the management control of criminal justice agencies. Appropriate up-to-date agreements shall be maintained and available during the audit. Similarly, satellite computers and manual terminals accessing the SYSTEM shall be under the management control of a criminal justice agency.
(240 IAC 5-2-10 (d), IDACS Manual Part I, Section C.)

11. In those instances where criminal justice agencies are utilizing equipment and personnel of a noncriminal justice agency for SYSTEM purposes, they shall have complete management control of the hardware and the people who use and operate the system.

    "Management control" means the authority to set and enforce:
    (1) priorities; (2) standards for the selection, supervision, and termination of personnel; and (3) policy governing the operations of computers, circuits and terminals used to process SYSTEM information insofar as the equipment is used to process, store, or transmit SYSTEM information.

    Management control includes, but is not limited to, the supervision of equipment, systems design, programming, and operating procedures necessary for the development and implementation of the computerized SYSTEM. Management control shall remain fully independent of noncriminal justice data systems and criminal justice systems shall receive priority service and be primarily dedicated to the service of the criminal justice community.
    (240 IAC 5-2-10 (d),(e),(f), IDACS Manual Part I, Section C.)

12. The criminal justice agency shall exercise management control with regard to the operation of the equipment by:
    (1) having a written agreement with the noncriminal justice agency operating the data center providing the criminal justice agency authority to select and supervise personnel;
    (2) having the authority to set and enforce policy concerning computer operations; and

(3) having budgetary control with regard to personnel and equipment, in the criminal justice agency.
(240 IAC 5-2-10 (g), IDACS Manual Part I, Section C.)

13. All computer sites accessing SYSTEM data shall have the security to protect against any unauthorized access to any of the stored data and/or the computer equipment including the following:
(a) All doors having access to the Central Processing Unit (CPU) room shall be locked at all times.
(b) A visitor's log shall be maintained of all persons entering the CPU area except those assigned to the area on a permanent basis. The visitor's name, date, time in, time out, agency represented and reason for visit.
(240 IAC 5-2-10 (j)(1)(A), IDACS Manual Part I, Section C.)

14. Since personnel at these computer centers have access to data stored in the SYSTEM, they shall be screened thoroughly under the authority and supervision of the IDACS committee or their designated representative. This screening shall also apply to noncriminal justice maintenance or technical personnel. The screening process shall consist of a character investigation, including fingerprints, for the purpose of establishing suitability for the position. Investigations shall consist of the gathering of information as the applicant's honesty, integrity and general reputation. Personal characteristics or habits, such as lack of judgment, lack of physical or mental vigor, inability to cooperate with others, intemperance, or other characteristics which would tend to cause the applicant to be unsuitable for this type of position, shall be considered sufficient grounds for rejection. Also, convincing information in an applicant's past history involving moral turpitude, disrespect for law, or unethical dealings shall be considered sufficient grounds for rejection. If any of the above facts are presented to the IDACS committee, a recommendation shall be made and presented to the state police superintendent for a final approval or disapproval decision.
(240 IAC 5-2-10 j (1)(B), IDACS Manual Part I, Section C.)

15. Computers having access to the SYSTEM shall have the proper computer instructions written and other built-in controls to prevent SYSTEM data from being accessible to any terminals other than authorized terminals. These instructions and controls shall be made available to the IDACS committee for inspection upon request.
(240 IAC 5-2-10 j (1)(D), IDACS Manual Part I, Section C.)

16. Computers and/or terminals (including mobile data terminals) having access to SYSTEM data shall maintain an audit of all transactions. This audit trail shall be maintained either manually by each agency or automated by the computer center. This transaction audit shall be monitored and reviewed on a regular basis to detect any possible misuse of SYSTEM data. This audit shall be made available to IDACS for inspection upon request.
(240 IAC 5-2-10 j (1)(E), IDACS Manual Part I, Section C.)

SECTION C
MISSING PERSON FILE
COMPLIANCE REQUIREMENTS

1. A missing person record shall be entered into IDACS and NCIC for the following reasons.
   a. Disability. A person of any age who is missing and under proven physical/mental disability or is senile, thereby subjecting himself/herself or others to personal and immediate danger.
   b. Endangered. A person of any age who is missing and in the company of another person under circumstances indicating that his/her physical safety is in danger.
   c. Involuntary. A person of any age who is missing under

circumstances indicating that the disappearance was not voluntary, i.e.,abduction or kidnapping.

d. Juvenile. A person who is missing and declared unemancipated as defined by the laws of his/her state of residence and does not meet any of the entry criteria set forth in a, b, c, or e.

e. Catastrophe Victim. A person of any age who is missing after a catastrophe.

f. Miscellaneous. A person above the age of emancipation who is missing and does not meet any of the criteria in a, b, c, or d can be entered into IDACS Files only.

(IDACS Manual, Part II Section F.)

2. A timely entry for a missing person is necessary to ensure maximum system effectiveness.

On a daily basis, all law enforcement agencies shall enter into the Indiana data and communication system (IDACS) computer the following: including information concerning extradition.

...(3) All information concerning runaways and missing persons, and missing children (as defined in IC 10-1-7-2), including information concerning the release of such persons to the custody of a parent or guardian.

The average entry delay of record(s) checked in the agency was _____ day(s). (See Data Quality Review).

(IC 5-2-5-12, IDACS Manual Part II, Section A.)

3. A record for a missing person may be entered in the Missing Person File provided the entering agency has documentation in its possession supporting the stated conditions under which the person is declared missing. This written documentation will aid in the protection of the individual's right to privacy. This documentation may be in the form of two separate documents, the officer's report and signed statement(s), or it may be only the officer's report if that report contains all of the following data:

1. The circumstances indicating reasons for considering the person as missing/runaway.

2. A statement indicating the relationship of the complainant to the missing person/runaway.
3. The signature of the complainant.

(IDACS Manual, Part II Section F.)

4. The ORI must account for all fields in the Missing Person File Ä Record Format. Ensure that all available data called for in the record format is entered when the entry is made. Missing data obtained at a later time should be promptly added through the use of a "modify" message.
(240 IAC 5-1-1 (b), IDACS Manual Part I Section D.)

5. The originating agency has the responsibility of immediately advising the locating agency concerning disposition of the individual when contacted about the location of the missing person.
(240 IAC 5-1-1 (d), IDACS Manual Part I Section D.)

6. Cancellation of a record is restricted to the agency that entered the record. A cancellation message is utilized when the entering agency determines that the record is invalid: for example, the parent or legal guardian of the missing juvenile withdraws the missing person report.
(240 IAC 5-1-1 (b), IDACS Manual Part I Section D.)

SECTION D
MISSING PERSON FILE
RISK ANALYSIS

Set aside for future developement.

SECTION E

VEHICLE FILE
COMPLIANCE REQUIREMENTS

1. A theft report must be on file for each entry in the Vehicle File.
   (240 IAC 5-1-2 (b), IDACS Manual Part I, Section D.)

2. A timely entry into the vehicle file is necessary to ensure maximum system effectiveness.
   On a daily basis, all law enforcement agencies shall enter into the Indiana data and communication system (IDACS) computer the following:
   (1) All information concerning any stolen or recovered property, including motor vehicles, firearms, securities, boats, license plates, and any other stolen or recovered property.
   The average entry delay of record(s) checked in the agency was _____ day(s). (See Data Quality Review).
   (IC 5-2-5-12, IDACS Manual Part II, Section A.)

3. The state of registry may enter a record for a vehicle stolen in another state when a test inquiry after a reasonable period of time discloses no record in NCIC. In this instance, the identity of the agency holding the theft report must be shown in the Miscellaneous (MIS) Field.
   (IDACS Manual Part II, Section H.)

4. A loaned, rented, or leased vehicle that has not been returned may not be entered in the file unless an official theft report is made or a filed complaint results in the issuance of a warrant charging embezzlement, theft, etc.
   (IDACS Manual Part II, Section H.)

5. If a felony vehicle is entered in the file, the whereabouts of the vehicle must be unknown.
   (IDACS Manual Part II, Section H.)

6. Partial license plate numbers must not be entered.

(IDACS Manual Part II, Section H.)

7. If a license plate number exceeds eight characters, enter only the last eight digits in the LIC Field. The full plate number must then be shown in the MIS Field.
(IDACS Manual Part II, Section H.)

8. When only one plate of a set is stolen or missing, a notation of this fact must be placed in the MIS Field of the entry.
(IDACS Manual Part II, Section H.)

9. A Locate transaction is used by a recovering agency to indicate on another agency's record that the vehicle has been located or recovered. This is the only transaction that an agency can take against another agency's record. Every time a recovery is made on a vehicle entered into the Wanted Files, it is the recovering agency's OBLIGATION to place a locate against the record. Failure to do so may result in a false arrest, detaining an innocent citizen, a civil law suit, or worse, since the locate data is shown on a hit response and would indicate to another agency receiving a hit that the record is probably no longer active.
(IDACS Manual Part II, Section H)

SECTION F
VEHICLE FILE
RISK ANALYSIS

Risk in the Vehicle File results from procedures that expose the agency to serious error due to the lack of sufficient care in maintaining records. The risk identified is a record entered in IDACS/NCIC

containing inaccurate and incomplete information, that is, information that will result in an erroneous hit or will prevent a proper hit from occurring. It is also defined as the risk of invalid information remaining in the System, that is, a record not being cleared when appropriate. Either risk is significant and may result in the arrest of an innocent citizen, the failure to arrest a sought-after criminal, or the death of an unsuspecting officer. Though this risk analysis has been written for the vehicle file, it can be easily used for other stolen property files as well.

1. Procedural Documentation for Entry

A. Written procedure and checklist 1
B. Written procedure or checklist 2
C. Well-defined oral procedures 5
D. No well-defined procedures 10

2. Basis for Entry

A. Officers report (written or oral), complainants written acknowledgment required 1
B. Officers report (written or oral) 2
C. Oral report by complainant, no follow up within twelve (12) hours 6
D. Oral report by complainant, no follow up 10

3. Quality Control Procedures

A. BMV checked, entry checked by a second person, message filed with supporting documentation 1
B. BMV checked, entry checked by a second person 2
C. Entry checked by a second person, entry message filed with supporting documentation 4
D. BMV checked, entry message filed with supporting documentation 5

E. Entry checked by a second person 6

F. BMV checked 7

G. Entry message filed with supporting documentation 9

H. No quality assurance measures 10

4. Validation Procedures

A. Agency has documentation to show that records are validated by contacting the appropriate complainant 1

B. Agency has a written policy requiring contact with the appropriate complainant 3

C. Agency has an oral policy that the complainant will be contacted as part of the validation process. Documentation does not exist to support these contracts 5

D. Agency does not comply with validation requirements 10

5. Hit Confirmation

A. Case report used for hit confirmation 1

B. Log book or card file used for hit confirmation 8

C. No satisfactory procedure 10

6. Documentation of Procedures for Clearing Entries

A. Written procedure and checklist 1

B. Written procedure or checklist 2

C. Well-defined oral procedures 5

D. No well-defined procedure 10

RISK LEVEL

LOW RISK - Less than 13 points

MODERATE RISK - 13 through 28 points

HIGH RISK - More that 28 points

Within each of the individual categories, risk is assessed as follows:

1-3 Low Risk

4-7 Moderate Risk, procedures should be reviewed and improved where possible

8-10 High Risk, procedures are insufficient and must be improved immediately

SECTION G
WANTED PERSON FILE
COMPLIANCE REQUIREMENTS

1. A Wanted Person record shall be entered into IDACS and NCIC for the following reasons.

   a. An individual (including a juvenile who will be tried as an adult) for whom a Federal warrant is outstanding.
   b. An individual (including a juvenile who will be tried as an adult) for whom a felony or serious misdemeanor warrant is outstanding.
   c. Probation and parole violators meeting the criteria in number 1 or 2 above.

   The following criteria applies to juveniles. Juvenile status is

determined by the laws of the state of residence of the parent, guardian, person or agency entitled to legal custody of such juvenile.

a. A juvenile who has been adjudged delinquent and is subject to the jurisdiction of the court making such adjudication, or to the jurisdiction or supervision of an agency or institution pursuant to an order of such court; and

   a) who has escaped from an institution or agency vested with the legal custody or supervision of such juvenile; or

   b) who has absconded while on probation or parole.

Juveniles who have been charged with the commission of a delinquent act that would be a crime if committed by an adult, and who have fled from the state where the act was committed. Entry of a record in this category is permitted only when a petition has been filed in a court of competent jurisdiction in the requesting state where the violation of criminal law is alleged to have been committed.
(IDACS Manual Part II, Section I.)

2. A timely entry into the wanted person file is necessary to ensure maximum system effectiveness.
   On a daily basis, all law enforcement agencies shall enter into the Indiana data and communication system (IDACS) computer the following:
   (2) All information concerning fugitives charged with any crime, including information concerning extradition.
   The average entry delay of record(s) checked in the agency was _____ day(s). (See Data Quality Review).
   (IC 5-2-5-12, IDACS Manual Part II, Section A.)

3. Before entering a record of a wanted person in IDACS/NCIC, the entering agency must attempt to determine, to the maximum extent possible, that extradition will be authorized if the individual is located in another state. For IDACS/NCIC purposes, extradition is the surrender by one state to another of an individual charged with or convicted of an offense outside its own territory and within the territorial jurisdiction of the other.

If at the time of entry there is a limitation concerning extradition of the wanted person, such information should be placed in the Miscellaneous Field of the record.

4. In many instances, however, no forecast of extradition can be made at the time the wanted person is entered in file because extradition is not a law enforcement decision. If at some future time the entering agency (ORI) learns that the individual definitely will not be extradited, the NCIC record must be cancelled, and re-entered into IDACS only.
   (IDACS Manual Part II, Section I.)

5. In instances where an agency is absolutely certain that the wanted person will not be extradited, the individual's record must not be entered in NCIC. Such records shall only be entered into the IDACS Files.
   (IDACS Manual Part II, Section I.)

6. Where there is an extradition limitation, it must be entered in the MIS field of the record.
   (IDACS Manual Part II, Section I.)

7. A temporary felony want record may be entered to establish a "want" entry when a law enforcement agency needs to take prompt action to apprehend a person (including a juvenile) who has committed, or the officer has reasonable grounds to believe has committed, a felony. This individual may seek refuge by fleeing across jurisdictional boundaries while circumstances prevent the immediate acquisition of a warrant.

   A temporary felony want record must be specifically identified as such. A warrant for the arrest of the individual must be obtained as soon as possible and thereafter, the temporary felony want record must be

either cancelled and a permanent wanted person record must be entered or the MKE must be modified to the permanent wanted person record. A temporary felony want record will be automatically removed from file after 48 hours.
(IDACS Manual Part II, Section I.)

8. Only the agency that holds the warrant may make an IDACS/NCIC entry. The only exception is that any criminal justice agency or regional dispatch center may act as holder of the record for another agency which has no telecommunications equipment.
(IDACS Manual Part II, Section I.)

9. A caution indicator should be added to the message key when it is known that an individual is armed and dangerous, has suicidal tendencies, has previously escaped custody, is a drug addict, or whatever is appropriate to the particular circumstances of the individual. The reason for the caution must be entered in the MIS field.
(IDACS Manual Part II, Section I.)

10. Any agency that apprehends or locates a person who is indexed in the NCIC Wanted Person File, except the agency that entered the record, must place a locate message on the wanted person record. When an agency receives a record or multiple records in response to an inquiry, the inquiring agency must contact the ORI of each record possibly identical with the person in question to confirm the hit. Following confirmation with the originating agency, a locate message must be transmitted for each record on file for the subject. A record should not be located if the locating agency is outside of the extradition limitations set forth in the record.
(IDACS Manual Part II, Section I)

11. An agency may enter a record for an unknown murderer in the name of "John" or "Jane Doe" using the homicide victim's descriptive data provided this type of warrant has been obtained. In such entries the victim's name should be listed as an alias, and his description and

personal identifiers, including date of birth, Social Security number, and driver's license number, should also be placed in the record as well as a statement in the Miscellaneous Field that the victim's personal identification may be in the possession of "John" or "Jane Doe."
(IDACS Manual Part II, Section I)

SECTION H
WANTED PERSON FILE
RISK ANALYSIS

Risk in the Wanted Person File results from procedures that expose the agency to civil suit due to the lack of sufficient care in maintaining records. The risk identified is a record entered in NCIC containing inaccurate and incomplete information, that is, information that will result in an erroneous hit or will prevent a proper hit from occurring. It is also defined as the risk of invalid information remaining in the System, that is, a record not being cleared when appropriate. Either risk is significant and may result in the arrest of an innocent citizen, the failure to arrest a sought-after criminal, or the death of an unsuspecting officer.

1. Procedural Documentation for Entry

A. Written procedure and checklist	1
B. Written procedure or checklist	2
C. Well-defined oral procedures	5
D. No well-defined procedures	10

2. Type of Warrants Entered

A. Felony only 1
B. Felony and serious misdemeanors 3
C. All warrants 10

3. Extradition Review

A. Formal review of extradition by appropriate authority, confirmed in writing 1
B. Formal review, but not confirmed in writing 2
C. Informal review 4
D. No extradition review 10

4. Basis for Entry

A. Written request accompanied by warrant 1
B. Original warrant maintained by agency 2
C. Written request, no warrant maintained 3
D. Oral request, confirmed in writing after entry 5
E. Oral request only 10

5. Quality Control Procedures

A. Criminal history records checked, entry checked by a second person, entry message filed with supporting documentation 1
B. Criminal history records checked, entry checked by a second person 2
C. Entry checked by a second person, entry message filed with supporting documentation 4
D. Criminal history records checked, entry message filed with supporting documentation 5
E. Entry checked by a second person 6
F. Criminal history records checked 7

G. Entry message filed 9

H. No quality assurance measures 10

6. Validation Procedures

A. Agency has documentation to show that records are validated by contacting the appropriate court or prosecutor 1

B. Agency has a written policy requiring contact with the appropriate court or prosecutor 3

C. Agency has an oral policy that the court or prosecutor will be contacted as part of the validation process. Documentation does not exist to support these contacts 5

D. Agency does not comply with the validation requirements 10

7. Hit Confirmation

A. Original Warrant verified, case report reviewed 1

B. Original Warrant verified 3

C. Case report reviewed 5

D. Card file or log book reviewed 7

E. No satisfactory procedures 10

8. Documentation of Procedures for Clearing Entries

A. Written procedure and checklist 1

B. Written procedure or checklist 2

C. Well-defined oral procedures 5

D. No well-defined procedures 10

RISK LEVEL

LOW RISK Less than 21 points

MODERATE RISK 21 through 34 points

HIGH RISK More than 34 points

Within each of the individual categories, risk is assessed as follows:

1-3 Low Risk

4-7 Moderate Risk, procedures should be reviewed and improved where possible

8-19 High Risk, procedures are insufficient and must be improved immediately

SECTION I
NON-TERMINAL AGENCY
ADMINISTRATIVE
COMPLIANCE REQUIREMENTS

AGENCY RECEIVES SERVICE FROM
_____

1. Agencies that enter records in IDACS/NCIC are responsible for their accuracy, timeliness, and completeness.
   (240 IAC 5-1-1 (b), IDACS Manual Part I Section D.)

2. Agencies that enter records in IDACS/NCIC are responsible for their accuracy, timeliness, completeness, and prompt removal. The accuracy of IDACS/NCIC records must be double-checked by a second party. That verification should include assuring that the available cross-checks,

e.g., VIN/License Numbers, were made, and that data in the record matches the data in the investigative report.
(240 IAC 5-1-1, IDACS Manual Part I, Section D.)

3. All IDACS user agencies shall validate, on a periodic basis, as prescribed to the user agency by IDACS, all IDACS wanted records entered on their authority. Validation of records shall be in conformity and compliance with rules set forth by IDACS.
   (b) Validation obligates the originating agency to confirm the record is COMPLETE, ACCURATE and is still OUTSTANDING or ACTIVE.
   (c) Validation is accomplished by reviewing the original entry and current supporting documents and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual. In the event the originating agency is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority shall make a determination based on the best information and knowledge available whether or not to retain the original entry on file. Validation procedures must be formalized and copies of these procedures must be on file for review during an IDACS or NCIC audit.
   (240 IAC 5-2-7, IDACS Manual Part I Section F.)

4. Terminal agency agrees to ensure that hit confirmation is available twenty-four (24) hours a day on records entered into the wanted files. This includes being able to provide a substantive response to an inquiry within ten minutes.
   (240 IAC 5-2-9, IDACS User Agency Agreement)

5. Likewise, the originating agency has an obligation to supply a substantive response within (10) minutes to the inquiring agency This response shall include a confirmation or denial of the wanted notice, or the length of time it will take to respond.
   (240 IAC 5-1-1, IDACS Manual Part I Section D, Part II Section A.)

IDACS AUDIT REPORT

1. AGENCY:			2. DATE:
3. ORI:	4. ID:	5. OPERATOR:	
6. COORDINATOR:		7. AGENCY HEAD:	
8. TERMINAL EQUIP:		9. CAPABILITY:	10. MDT'S:
11. LOCATION:			
12. SECURE:	13. SERVICE HOURS:	14. INSPECTION TYPE:	

DIAGRAM

NORTH ☐

15. REMARKS _____

16. WARNING OR NOTICE OF VIOLATION:

17. REVIEWING AGENCY OFFICIAL: _____
(PRINT NAME) (SIGNATURE)

18. IDACS SECURITY OFFICER:

ADMINISTRATIVE COMPLIANCE REQUIREMENTS

A1.
(1). COMPLIANCE: IN OUT NA
(2). COMPLIANCE: IN OUT NA
(3). COMPLIANCE: IN OUT NA
(4). COMPLIANCE: IN OUT NA
(5). COMPLIANCE: IN OUT NA
(6). COMPLIANCE: IN OUT NA
(7). COMPLIANCE: IN OUT NA

A2. COMPLIANCE: IN OUT NA
(See Data Quality Review)

A3. COMPLIANCE: IN OUT NA

A4.
a. COMPLIANCE: IN OUT NA
b. COMPLIANCE: IN OUT

A5. COMPLIANCE: IN OUT NA

A6. COMPLIANCE: IN OUT NA

A7. COMPLIANCE: IN OUT NA

A8. COMPLIANCE: IN OUT NA

A9. COMPLIANCE: IN OUT NA

A10. COMPLIANCE: IN OUT NA

A11. COMPLIANCE: IN OUT NA

A12. COMPLIANCE: IN OUT NA

If OUT of compliance, narrative required on page 1.

SYSTEM SECURITY COMPLIANCE REQUIREMENTS

B1. COMPLIANCE: IN OUT NA

B2. COMPLIANCE: IN OUT NA

B3. COMPLIANCE: IN OUT NA

B4. COMPLIANCE: IN OUT NA

B5.
(1) COMPLIANCE: IN OUT NA
(2) COMPLIANCE: IN OUT NA
(3) COMPLIANCE: IN OUT NA
(4) COMPLIANCE: IN OUT NA

B6. COMPLIANCE: IN OUT NA

B7. COMPLIANCE: IN OUT NA

B8. COMPLIANCE: IN OUT NA

B9. COMPLIANCE: IN OUT NA

THE BELOW QUESTIONS FOR COMPUTER CENTERS AND DISPATCH CENTERS ONLY

B10. COMPLIANCE: IN OUT NA

B11. COMPLIANCE: IN OUT NA

B12.
(1) COMPLIANCE: IN OUT NA
(2) COMPLIANCE: IN OUT NA
(3) COMPLIANCE: IN OUT NA

B13.
(a) COMPLIANCE: IN OUT NA
(b) COMPLIANCE: IN OUT NA

B14. COMPLIANCE: IN OUT NA

B15. COMPLIANCE: IN OUT NA

B16. COMPLIANCE: IN OUT NA

If OUT of compliance, narrative required on page 1.

NON-TERMINAL AGENCY ADMINISTRATIVE COMPLIANCE REQUIREMENTS

I1. COMPLIANCE: IN OUT NA

I2. COMPLIANCE: IN OUT NA

I3. COMPLIANCE: IN OUT NA

I4. COMPLIANCE: IN OUT NA

I5. COMPLIANCE: IN OUT

I6. SERVICED BY: _____

If OUT of compliance, narrative required on page 1.

MISSING PERSON FILE

C1. COMPLIANCE: IN OUT NA

C2. COMPLIANCE: IN OUT NA
(See Data Quality Review)

C3. COMPLIANCE: IN OUT NA

C4. COMPLIANCE: IN OUT NA

C5. COMPLIANCE: IN OUT NA

C6. COMPLIANCE: IN OUT NA

If OUT of compliance, narrative required on page 1.

RISK ANALYSIS: D1. = _____ D2. = _____ D3. = _____ D4. = _____ D5. = _____ D6. = _____

D7. = _____ D8. = _____ TOTAL RISK = ____ LEVEL = _____

VEHICLE FILE

E1. COMPLIANCE: IN OUT NA

E2. COMPLIANCE: IN OUT NA
(See Data Quality Review)

E3. COMPLIANCE: IN OUT NA

E4. COMPLIANCE: IN OUT NA

E5. COMPLIANCE: IN OUT NA

E6. COMPLIANCE: IN OUT NA

E7. COMPLIANCE: IN OUT NA

E8. COMPLIANCE: IN OUT NA

E9. COMPLIANCE: IN OUT NA

f OUT of compliance, narrative required on page 1.

RISK ANALYSIS: F1. = _____ F2. = _____ F3. = _____ F4. = _____ F5. = _____ F6. = _____

TOTAL RISK = ____ LEVEL = _____

WANTED PERSON FILE

G1. COMPLIANCE: IN OUT NA

G2. COMPLIANCE: IN OUT NA
(See Data Quality Review)

G3. COMPLIANCE: IN OUT NA

G4. COMPLIANCE: IN OUT NA

G5. COMPLIANCE: IN OUT NA

G6. COMPLIANCE: IN OUT NA

G7. COMPLIANCE: IN OUT NA

G8. COMPLIANCE: IN OUT NA

G9. COMPLIANCE: IN OUT NA

G10. COMPLIANCE: IN OUT NA

G11. COMPLIANCE: IN OUT NA

If OUT of compliance, narrative required on page 1.

RISK ANALYSIS: H1. = _____ H2. = _____ H3. = _____ H4. = _____ H5. = _____ H6. = _____

H7. = ____ H8. = ____ TOTAL RISK = ____ LEVEL = _____

DATA QUALITY REVIEW

1. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

2. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

3. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

4. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

5. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

6. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

7. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

8. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

9. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

10. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

11. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

12. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

13. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

14. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

15. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____

16. IDX_____ OCA_____ ENTRY DELAY____DAYS CORRECTIONS/_____